Team Exercise #3

Web Applications

Exercise: May 13 & 15, 2019
Report Due Date: May 20, 2019 at 5:15 p.m.

Introduction

This exercise expands on what we did with the first two exercise. The big differences? Web servers are now required to host fully functional web applications.

This document is split into two sections- the first discusses the elements common to all exercises, while the second describes the elements specific to this exercise.

Common Elements

Your team has been tasked with building the computer network infrastructure for a new company. The company is organized into a sales staff, a corporate staff, a production staff, a group of IT admins (you!) and of course, the CEO.

You have the following build requirements:

- You must build the network (described below), including accounts for all of the users.
- The required services must remain up during the course of the exercise.
- You have received various sets of confidential corporate data. This data must be available to authorized users, and only to authorized users.

Once the exercise starts:

- Automated tools will scan your network to validate that the required services are up.
- You must determine the IP addresses and services provided by each of the other teams.
- You may attempt to attack the networks of the other student teams.
- A group of professionals (the Red Team) will ~~attempt to~~ penetrate your network.

Once the exercise concludes, you need to determine:

- Was the team successfully attacked? [HINT: The correct answer is going to be "yes".]
- For each successful attack, determine:
  - How was the attack performed?
  - What access was gained by the attackers?
  - What data, if any, was exfiltrated by the attackers?
  - Who were the attackers? Weak identification would be to determine an IP address. Strong identification would be to determine the team. Perfect identification would be to determine the person.
- Identify any elements of the network that did not function correctly (or at all). Determine the cause of the malfunction.

1 Team Network

Each team has five networks to build. The first network is the corporate network, the second is the sales network, the third is the production network. The team will have a network in the cloud, so the team will not have physical access to these systems. The last network is the team's attack network.

1.1 System Re-Use

Linux systems may be any of the distributions provided in class (CentOS 6.2, 6.5, 6.8, 7.0; Mint 13, 17.1, 18.1; Ubuntu 12.04, 14.04, 16.04). No single distribution may be used twice by the team unless every other distribution has already been used. For example, the team may not use a second CentOS 7.0 system in the network if there is no system that is using Ubuntu 16.04.

Windows server systems may be any of the 4 versions provided in class (Windows Server 2008 R2, 2012, 2012 R2, 2016). No single version may be used twice by the team unless every other version has already been used. The team cannot use a second Windows 2016 server if the team does not have a Windows 2008 R2 server in the network. Care should be taken when installing Active Directory to ensure that the functional level of the domain allows all of the server to join the domain.

Windows desktop systems may be any of the 4 versions provided in class (Windows 7 SP1, 8, 8.1, 10). No single version may be used twice by the team unless every other version has already been used. No single version may be used three times by the team unless every other version has already been used twice.

1.2 Networking

The class B network 10.0.0.0/16 is reserved for use in class as a demonstration network and is not to be used by student teams during the exercise. The network is further subdivided into class C networks:

- **10.0.0.0/24** = 10.0.0.1 - 10.0.0.253 (gateway 10.0.0.254) is assigned by DHCP to the physical workstations in the class.
- **10.0.1.0/24** = 10.0.1.1 - 10.0.1.253 (gateway 10.0.1.254) is assigned via DHCP to virtual machines that are set up in class.
- **10.0.x.0/24** = 10.0.x.1 - 10.0.x.253 (gateway 10.0.x.254) for $x = 2, 3, 4, 5$ are available for students to use when building systems for practice that are not intended for use in an exercise. Team 1 may use 10.0.2.0/24, Team 2 may use 10.0.3.0/24, Team 3 may use 10.0.4.0/24 and Team 4 may use 10.0.5.0/24.
- **10.0.6.0/24** = 10.0.6.1 - 10.0.6.253 (gateway 10.0.6.254) is used by the instructor. Exercise Control lives at 10.0.6.250, and is described in more detail later.

Each team is assigned class C networks in the class B network 10.x.0.0/16 (gateway 10.x.254.254) where $x = 1, 2, 3, 4$ is the team number. The precise networks are indicated in your team specific handout. Each system is assigned a random IP address, also specified in your team specific handout.

Host names are either *.corp.teamx.tu or *.sales.teamx.tu or *.production.teamx.tu for $x = 1, 2, 3, 4, 5$.

Each team's remaining class C networks and each team's host names are unknown to competing teams at the start. During the attack portion of the exercise, teams need to determine the architecture of the network for each other team.

The IP address of the primary DNS server for each team will be provided.

Oh yes, before I forget. The Red Team has been assigned lots and lots addresses in 10.x.0.0/16 for $x = 1, 2, 3, 4, 5$ that don't conflict with team addresses. Which ones are theirs, and which ones belong to student teams? I just smile at the thought. I hope they set up some vulnerable systems for you to attack, just so they can use them as a channel back to your own attacking systems. That would be fun.

1.3 Users

A list of employees in your company has been provided. Given a user, form the user name as the first letter of the first name followed by the full last name, all in lower case. For example, the user Ned Stark has the user name nstark.

Users are assigned one of five roles:

- The CEO
- IT Staff
- Corporate Staff
- Sales Staff
- Cloud Staff
- Production Staff

The following rules are in effect:

- The CEO must be able to log on to the CEO workstation, as well as the Sales workstations, the Corp workstations, and the Production workstations.
- The IT Staff must be able to log on to any system. They should be domain admins and allowed to `su` to root on any Linux system.
- The Corporate staff must be able to log on to any Corp workstation.

- The Sales staff must be able to log on to any Sales workstation.
- The Production staff must be able to log on to any Production workstation.

There are many possible architectures that satisfy these requirements; you are free to choose how to ensure the requirements are met.

You may set up other accounts as you see fit.

1.4 Passwords

The passwords on your systems must be selected from a finite (and small) list of allowable passwords. This restriction makes brute-force attacks on your passwords feasible in the time allotted for the exercise. If you set up additional accounts beyond those required for the exercise, they must use one of these passwords.

The collection of all allowable passwords is available on exercise control. They are formed from 9396 common 8 letter words, prefixed with the string "P1#".

If your systems are not hardened to protect against brute-force attacks, they will fall.

1.5 Confidential Data

Each team is provided with three sets of confidential data- a set of account data, a set of personal data, and a set of account data. The account data `TeamxAccount.csv` has four fields: User name, IP Address, Referrer, and Password. The personal data `TeamxPersonal.csv` has seven fields: Name, Address, City, State, Company, Job Title, and Social Security Number. The financial data `TeamxFinancial.csv` has seven fields: Name, Address, City, State, Credit Card number, Credit Card type, and Balance.

The employee directory `TeamxEmployees.csv` includes the first name, last name, corporate role, email address and phone number of each employee; these match the user names for your company. It is not quite as confidential as the other three files, but still not something that is meant to be publicized. Note also that this employee directory is what you use to determine the account names of the users on your network.

These `.csv` files can be read and written with a text editor; they can also be opened in a spreadsheet. A copy of LibreOffice is available on all Windows and Linux systems; these can be used to edit these files.

1.6 Defensive Techniques

You may want to harden your systems to make it more difficult for attackers.

1.6.1 Firewall Rules

You may use whatever firewall rules you wish on your hosts.

Any or all inbound connections may be blocked. However, you are responsible for the result, so if Nagios cannot reach your system because of your firewall rule settings, then the problem falls on your team.

Blocks on traffic must block all IP addresses or none. You cannot block inbound traffic based on the source IP address or membership in a windows domain. These rules on blocking inbound traffic also apply to other tools, like `hosts.allow` and `hosts.deny`.

Though you can configure firewalls to block outbound connections, you may not block all ports. In particular, the following ports must always open for outbound traffic to arbitrary IP addresses:

TCP / 20	TCP / 22	TCP / 110	TCP / 143	TCP / 989	TCP / 993
TCP / 21	TCP / 80	UDP / 123	TCP / 443	TCP / 990	TCP / 995

You can block TCP / 4444 if you wish.

Exceptions Some ports or protocols are such that if they are not protected from the Internet, they are likely to be compromised. Teams are free to block access to UDP/53, TCP/53, TCP/137, TCP/139, TCP/445 by IP address. No other ports are allowed to be blocked by IP address

Countermeasures. If a team can provide compelling evidence of an attack more threatening than a simple port scan to the instructor from a known IP address, then the team may receive permission from the instructor to block communication to and/or from that IP address.

The team may also use defensive tools like SSHGuard to automatically single IP addresses for a short period of time based on characteristics of their network traffic.

1.6.2 Local Policies, Group Policies, and Software Restrictions

The use of Group Policies or Local Policies to secure systems is encouraged. However all users must have the right to

- Visit arbitrary web pages.
- Run any already installed program that does not require elevated privileges; this includes web browsers, command shells, Java, Adobe Reader, and Adobe Flash. Blocking network connections to/from these programs or otherwise interfering in how they run is not permitted.
- Download and run any program that does not require elevated privileges.

You may also set up and use Software Restriction Policies or AppLocker. Software Restriction Policies and AppLocker restrict where programs can be run; they cannot be used to block *all* downloaded programs. Moreover, we assume that the user is smart enough to know where programs can be placed to run. If you receive an email asking you to download and run a program, your settings must allow the user to do just that.

1.7 Specifications

Teams will be provided additional documents that complete these specifications. These include:

- The file "DNS", which provides the IP address for the primary DNS server for all four student teams.
- The file "WebServers" which provides the names of the web servers of all four student teams.
- The file "TeamxNetwork.csv" (for $x = 1, 2, 3, 4$) that provides for each non-attacking system its name, IP address, role, OS, and external services.
- The file "instructions" that explains the requirements for the required external services and roles. These are checked by Exercise Control.
- The file "TeamxAdmin.csv" (for $x = 1, 2, 3, 4$) that provides your email accounts and paswords for Exercise Control.
- The confidential files "TeamxAccount.csv", "TeamxPersonal.csv", "TeamxFinancial.csv", and "TeamxEmployees.csv" (for $x = 1, 2, 3, 4$).

2 Exercise Control

A system is provided by the instructor for exercise control; it is named disc.classex.tu, and is located at 10.0.6.250. Exercise control is strictly out-of-bounds for all attacks. Traffic from exercise control should be considered trusted.

2.1 DNS

Exercise control provides a DNS server (TCP/53, UDP/53) for the `classex.tu` namespace and the 10.0.6.0/24 address space. Exercise control forwards DNS requests for all sales, corp, and production domains and corresponding IP address spaces to a DNS server for that team. If these DNS servers are down, these requests will fail. Teams are permitted to configure their internal DNS systems to forward requests for other teams to exercise control; they would then be forwarded to the proper team DNS server for ultimate resolution.

2.2 Service Checks

Exercise control runs a Nagios server. This tool checks to see what hosts are up and responsive and what services they are providing. This information is used for grading. Teams can see the status of the systems on their network through Nagios. Log in to the Nagios system on exercise control, using the account teamxadmin and the password provided; this is the same account and password used for your email account on Exercise Control.

Service checks are different for different services. Some may check that a service is listening, others may authenticate to the service, and others may verify the integrity of the data.

Service check failures can occur for any number of reasons, sometimes unrelated to the service being checked. For example, if SSH is being checked on host.teamx.tu and your DNS server does not have the correct record for host.teamx.tu, then the service check will fail. Failure of a DNS system generally causes a cascade of service check failures, so be sure that DNS is fully functioning first and at all times.

It is your responsibility to ensure that all service checks are passed. This is a key component of the exercise!

Nagios provides telemetry for all of its checks. These are sent via the syslog protocol to the system listed as the default log server for your network. If that server is properly configured to accept remote log entries, you will be provided detailed information whenever a Nagios check fails. Messages are sent using local5.error for easy filtering on your end.

Exercise control provides detailed help on each Nagios check; this includes providing you with the raw source code that is being used to perform the check, as well as an enumeration of some possible failure models for the check.

2.2.1 Accounts and Passwords

Nagios selects particular accounts to make various checks; these accounts may have any of the various roles (*e.g.* CEO, IT Staff). To authenticate to your systems, Exercise Control needs to be informed of the password for each of your accounts; this is done through a web page on Exercise Control itself. Log on using your teamxadmin account and password to make these changes.

Until the proper password is entered, Exercise Control will use the default password "password1!" for all checks that require a password; this means that it is likely that your checks will fail. This would be bad.

Only passwords from the allowed list of legal passwords can be used.

2.3 Email

Exercise control provides in-class email services.

Email can be checked from a webmail interface at `https://disc.classex.tu/mail`. Exercise control provides IMAP (TCP/143, TCP/993) and POP3 (TCP/110, TCP/995) servers, with and without SSL to receive mail. Exercise control provides authenticated SMTP with SSL (TCP/25) for the sending of mail. Each provided image includes an email client (Thunderbird or Evolution). These can easily be configured to read and send email.

Each team has two email accounts. The account teamxadmin@classex.tu is used for all administrative communication. It must be actively monitored during the exercise. An email has already been sent to that account providing electronic files for your network.

The second email account is not associated with a team name. A team that wishes to send an email to another team without making it quite so obvious which team sent the message can use this account.

The red team has multiple email accounts, including redteam@classex.tu.

All email to/from the instructor comes from svimes@classex.tu.

Passwords for the email accounts do not come from the (short) list of authorized passwords. They may not be changed during the exercise. The mail server itself is part of Exercise Control, and so is out-of-bounds for attack. However, if an attacker obtains the email password of a team account, they may use those credentials to send / receive email. This is most amusing.

2.4 Web Server

Exercise control provides a web site `http://disc.classex.tu` with the latest and most up to date information about the services provided by exercise control.

That site includes

- The public certificate for the CA that was used to sign all SSL certificates used by exercise control (*e.g.* https, IMAP/SSL, POP3/SSL, SMTP/SSL). It is recommended that you import this certificate into your clients (browsers, email clients) as appropriate.
- The SSH public key used for various SSH service checks.
- The list of all possible passwords used for systems other than those on/for exercise control.

2.5 Pastebin (Stikked)

Multiple companies have seen their private corporate data end up on anonymous public sites like Pastebin. (Sony-I am looking at you!) Exercise control provides Stikked at `http://disc.classex.tu/stikked/`, which is an open source equivalent to Pastebin. Teams that are able to successfully obtain confidential information from another may post the result to site to prove the success of the attack. Teams with others' confidential data are permitted to negotiate with the source for additional consideration in lieu of posting some or all of the confidential data.

Teams that see confidential data posted to Stikked will be required to explain how it got there. In detail.

3 Service Checks

Once the exercise commences, the team's first responsibility is to ensure that their network remains up and functioning. Service checks are made by Nagios roughly once every few minutes. Failing multiple checks will result in a significant loss of score; this is explained in detail in §7: Grading.

4 Offense

Teams are free to engage in offensive activity aimed at other teams, with some caveats.

- All offensive activity must occur during the class time set aside for the live exercise. No attacks are permitted before the live exercise begins, after it ends, or during the time between the live exercise nights.
- Students are not allowed to download, modify, copy or even touch the systems of students on other teams.
- The only allowable targets are the virtual machines of other teams. Attacks may not target the physical hosts, exercise control, networking, or systems of the Red Team.
- Students will act at all times with respect towards one another.
- No offensive activity that disrupts the learning environment is permitted. This can include a range of activities, from deleting logs to poor man-in-the-middle attacks to simply obnoxious behavior. If you are unsure, check with Prof. O'Leary or Prof. Hornberger before launching the attack.

4.0.1 Denial of Service Attacks

Denial of service attacks against BIND DNS servers are explicitly prohibited. This includes the TKEY (CVE 2015-5477) attack, and the TSIG/Buffer.c (CVE 2016-2776) attack. Why? The Internet Systems Consortium, which produces BIND, has publicly stated that there are no workarounds or configurations that protect against this attack other than patching to an updated version. Since updating BIND is prohibited in class- well, there you are. Both of these attacks leave the IP address of the offending system in the log and they are trivial to detect. Their use in the class by a team will result in a massive grade penalty.

4.1 E-Mail

Many attacks require a user on the target system to perform some activity- viewing a web page, or running a program. Students and the Red Team may send a message via e-mail asking for a user on another team to

- Visit a provided web site,
- Open a provided file, or
- Run a provided program.

Students and the Red Team may require the action to be taken by a particular user- either

- The CEO
- A member of the sales staff, or
- A member of the corporate staff, or
- A member of the production staff.

If no account or group of users is specified, then the team receiving the request may select any user capable of performing the task.

Students and the Red Team may specify that the action be taken on a particular workstation, or on a workstation with a particular operating system / version (*e.g.* Linux, or Windows 8). If no workstation is selected, then the action must be taken on any appropriate workstation.

Students and the Red Team may specify that a particular browser and version is to be used.

A team that receives a request must make a good faith effort to comply with the request. Once the request is completed, the team must reply to the requester stating either that the requested action has been taken, or stating that it is impossible (and justifying that claim). The team does not have to report the results of the activity. If the program crashes, or the browser hangs, well, that sometimes happens to real attackers too. We don't tell them what went wrong, do we?

Oh- and for all of the prospective classroom lawyers, if you are sent a Windows executable, the you need to run it on a Windows system. Running on Linux with Wine is (a) clever and (b) prohibited. Don't get me started about

running 64 bit executables on 32 bit systems, then claiming a crash. Another favorite is saying the program can't be run on Linux because when you saved the file you did not set the executable bit in the file permissions. Oh how clever. Go execute that file before I get my gradebook and red pen out. Remember- you must make a *good faith effort* to comply with these messages. If a team does not make such an effort, the Red Pen of Judgment will reduce your grade much more than if the attack is successful.

In all cases, be sure to either copy svimes@classex.tu on the messages to the target and any resulting replies. This helps with grading!

Teams may not deliberately re-set, re-start or re-boot a system just because another team asked it to perform an action.

4.2 Records

During the exercise, you must keep a careful record of what activity you perform on the network. This includes detailed summaries of all scans, probes, and attacks. This information should be included in a table or tables in your final report. These records are required if a student team wishes to receive credit for a successful attack.

5 After the Exercise

After the exercise is complete, each team writes a single team report. The final report will be neat, organized, and well-written. It will contain:

- A complete summary of all of the machines placed on the network, whether required or not.
- An evaluation of the functioning of your network.
- The results of your reconnaissance and any attacks attempted.
- The analysis of any attacks performed against your network. If confidential data was exfiltrated from your network, explain how it happened. (In detail.)

The report must also specify the responsibilities and activities of each team member in reasonable detail.

Exercise 3 Specifics

The live exercise will run from 5:00 – 6:15 on May 13. On May 15, the exercise runs from 5:15 – 7:15. A single team report is due at 5:15 on May 20.

6 Team Network

The corporate network includes:

- One Linux BIND DNS server; this also runs SSH.
- A Linux file server running Samba and (anonymous) FTP.
- A Windows workstation with RDP.
- A phpMyAdmin web application on Linux systems; one system with the web server and a second with the database.
- A Joomla! 3.4 web application on Windows systems; one system with the web server and a second with the database.

The sales network includes:

- One Linux BIND DNS server; this also runs SSH.
- A Linux log server for the entire organization.
- A Linux workstation with SSH.
- A phpMyAdmin web application on Windows systems; one system with the web server and a second with the database.
- A Wordpress 4.0 web application on Linux systems; one system with the web server and a second with the database.

The production network includes:

- A domain controller running active directory and DNS for the production domain.
- A Windows file server
- A Windows worsktation
- A Wordpress 3.5 web application on Windows systems; one system with the web server and a second with the database.
- A Joomla! 3.6 web application on Linux systems; one system with the web server and a second with the database.

The cloud network will be run on the class ProxMox server. Students will not have physical access to the system, but instead must configure everything remotely. The cloud network includes:

- A domain controllers running active directory and DNS for the cloud domain
- A Windows file server.
- A Wordpress 4.3 web application on Linux systems; one system with the web server and a second with the database.
- A Joomla! 3.3 web application on Windows systems; one system with the web server and a second with the database.

Windows servers on the cloud should not have an installed graphical user interface (GUI). The use of Windows Server 2008 R2 is not recommended. It is recommended (but not required) that the team configure one or more of workstations with the needed remote server administration tools. The web interface to the cloud server may be disabled during the exercise.

The attack network consists only of attacking systems; the number and configuration is at the team's discretion.

7 Deadlines & Requirements

The network must be complete and functional prior to the start of the exercise at 5:00 on May 13. System and network performance is graded beginning promptly at the start of the exercise.

Each student must take primary responsibility for four or more systems, including at least one complete web application.

8 Grading

Grading for the exercise is broken down into five components:

8.1 (30 points) Host Performance

Each host is graded by how well it functioned over both exercise dates:

- (10 points) The system and its services performed perfectly.
- (9 points) The system and its services were consistently available.
- (6 points) The system and its services were occasionally disrupted.
- (3 points) The system and its services were often available.
- (0 points) The system and its services were usually unavailable.

The nature of the exercise is such that perfect performance is rare. A system or service that is down for 15 minutes or more is not consistently available. A system that is down 45 minutes or more is worse than occasionally disrupted. A system that is down for for a full night is considered usually unavailable- this means that the responsible student will receive a score of zero for that system. (Ouch).

Most systems have multiple scored services, the lowest score is used.

There may be times when scoring is disrupted, either due to network activity or professor misconfiguration of the Nagios engine. Students are not accountable for these disruptions.

Each student is scored for the three systems for which they were responsible. A student responsible for four systems receives the scores for the highest three systems provided all systems were at least often available. Otherwise the student receives the average of all systems.

Though host scores are per-student, this is a team project, and students can have their scores affected by the actions of their teammates. For example, an SSH server built by student A may be reported as down because of an error in the DNS configuration of student B. Student A remains responsible for the score.

8.2 (15 points) Network Design

The report should explain the design of the network.

- This should include diagram(s) of the network as built by the students, including an explanation of how the network was divided between the physical hosts.
- This should include an explanation of the networking used behind the firewall(s), including IP addressing and netmasks.
- The network checked by Nagios is not meant to complete, as it does not include backups for key services or intrusion detection systems. The report should explain what additional systems, if any, were added to the required list, and explain their purpose.
- A summary of the firewall configuration should be provided.

8.3 (0 points + bonus) Reconnaissance & Attack

Students are encouraged take offensive action against other teams. Bonus points are available:

- (1 point/system up to 5 points) Gaining a shell on a remote system. [Provide a screenshot.]
- (2 points/system up to 10 points) Gaining root/administrator access on a remote system. [Provide a screenshot.]
- (5 points/domain up to 15 points) Gaining domain administrator access. [Provide a screenshot.]
- (1 point/file) Gaining access to team confidential data. [Include a portion of the file in the report.]

Attackers generally do not want to be caught. These scores are subject to modification based on whether your actions are detected.

- (Attack score $\times 2/3$) Attack is detected by defenders.
- (Attack score $\times 1/3$) Attack is detected and the defender correctly identifies the source.

8.4 (20 points) Defense

Each team starts with 20 points, and can lose points due to successful attacks:

- (2 points/system up to 10 points) Opponent gains a shell on a system.
- (4 points/system up to 20 points) Opponent gains root/administrator access.
- (15 points) Opponent gains domain administrator access.
- (1 points/file) Opponent gains access to confidential file.
- (1 points/file) Opponent dumps some or all of a confidential file in public.

It is possible for this score to drop below zero.

8.5 (20 points + bonus) Analysis

Students should analyze the results of the exercise. Explain what worked, what did not work, and explain why it did occurred as it did. The quality of the analysis is worth 20 points. Of particular importance in the quality of the analysis is the correct use and integration of data from multiple sources. Claims of what occurred should be supported by data from multiple sources. The analysis should also take place at the network and team level, rather than at the student or system level.

An example of poor analysis would be to claim that a particular system was "hacked" by an unknown attacker based on a single odd entry in the log. An example of good analysis would be to claim that a particular system was compromised by at attacker with a known IP address; this is known because the attacker first ran an NMap scan of the network (with supporting documentation) then served a known exploit (with supporting documentation) that resulted in a callback to that IP address (with supporting documentation).

Points lost to a successful attack (§7.3) can be regained through analysis. If the team correctly identifies an attack, one half of the lost points are recovered. If the team is also able to identify the source of the attack, the remaining one half of the lost points are recovered.

To gain these points back, the explanation in the report must be clear and unambiguous, stating what occurred and how. The burden of proof is on the defending team, and claims supported with weak or no evidence will not receive points back, even if the claim is correct.

Claims of a successful attack that are not actually the result of an attack cause the team to lose additional points at the same rate as §7.3. Teams that make many incorrect claims can end with a score below zero.

8.6 (15 points) Report Quality

The quality of the written report is graded according to a range of criteria

- Did the report communicate their ideas clearly and effectively?
- Is the report cleanly organized?
- Is the report one coherent whole?
- Does the report contain all of the required elements?
- Does the report make effective use of graphics and tables?
- Is the work in the report all original?
- Does the report include a summary of all of the computers on the network?
- Does the report contain a complete summary of all network activity performed against other teams?
- Does the report contain an evaluation of the functioning of the team's network?
- Does the report well summarize the results of the teams reconnaissance activity?
- Does the report contain an analysis of the logs?
- Does the report correctly identify who was responsible for each system?
- Did the team members summarize the roles each team member played?

8.7 Team Score

If in the judgment of the instructor different team members made substantially different contributions, then members of the team may be assigned different grades.